Department of Veterans Affairs

Monthly Report to Congress On Data Incidents

August 2010

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370736	Privacy	VISN 03 New York, NY	8/2/10	8/5/10		High	1
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/2/2010	INC000000104949	N/A		N/A		N/A	0

Incident Summary

The VA Medical Center Release of Information (ROI) employee sent the medical records of Veteran A to Veteran B. Veteran B returned the opened envelope and all documents to the ROI department. The documents contained the name, address, social security number and PHI for Veteran A.

Incident Update

08/03/10:
Veteran A will receive a letter offering credit protection services.

NOTE: There were a total of 20 Mis-Mailed incidents this reporting period. Because of repetition, the other 19 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The credit protection letter was mailed to Veteran A..

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370745	Privacy	VHA CMOPGREAT LAKES, IL	8/2/10	8/31/10		Moderate	0

Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/2/2010	INC000000104960	N/A		N/A		N/A	1

Incident Summary

Patient A received a prescription by mail that was intended for Patient B. Patient B's name and type of medication were compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP employee mail preparation error. The employee placed an incorrect label on the package. The employee will be counseled and retrained in proper mail manifest procedures.

Incident Update

08/03/10:
Patient B will receive a letter of notification.

NOTE: There were a total of 2 Mis-Mailed CMOP incidents out of 5,640,115 total packages (8,403,191 total prescriptions) mailed out for this reporting period. Because of repetition, the other 1 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The notification letter was mailed on 08/26/20 for Patient B.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370812	Missing/Stolen VA Resources	VISN 22 Loma Linda, CA	8/2/10	8/10/10		Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/2/2010	INC000000105036	N/A		N/A		N/A	

Incident Summary

Sometime between 6:30 PM on 08/01/10 and 8:00 AM on 08/02/10, an off-site VA location was broken into and 13 computers were stolen. Eight of the PCs were locked to the desks and the cables were cut. Five of the PCs were new and still in their boxes. The Facility CIO (FCIO) verified that none of the PCs stored any PII or PHI and all were newly imaged. This is a new facility prepared for use by additional staff. The VA Police and the local San Bernardino Sheriff's Department are involved and investigating.

Incident Update

08/24/10:
The computers were to be used for normal administrative and clinical work. There was no PII or PHI stored on them.

Resolution

The following actions have been taken. All doors have been re-keyed. Contractors no longer have direct access. All contractors will now be escorted by VA personnel. Effective COB 08/02/10, a working alarm system was installed.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370824	IT Equipment Inventory	VISN 22 Long Beach, CA	8/2/10	9/6/10		Moderate	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/2/2010	INC000000105043	N/A		N/A		N/A	

Incident Summary

During inventory, it was determined that a non-encrypted VA laptop was missing from Prosthetics. The laptop used Computer Aided Design software and was used to design prosthetic items. The user reports that no PII/PHI was stored in the laptop.

Incident Update

08/11/10:
The laptop was not encrypted. It was purchased by Prosthetics in 2008. OI&T/IRM was not aware of the existence of the laptop until it was reported missing. The laptop was not used for patient care. It was used as a teaching tool on dummy test cases.

NOTE: There were a total of 1 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other # are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The VA Police Report and Report of Survey were completed.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0371091	Privacy	VISN 07 Columbia, SC	8/3/10	8/11/10		Low	0
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/3/2010	INC000000105196	N/A		N/A		N/A	1

Incident Summary

On 07/27/10, Veteran A reported to the Outpatient Pharmacy to pick up his medication and was also issued Veteran B's medication. Veteran A returned to the Dorn VA Medical Center Outpatient Pharmacy window to bring back Veteran B's medication on 07/28/10. No medication was taken. The Privacy Officer was notified by the Pharmacist on 08/02/10. The information disclosed included Veteran B's full name and type of medication. The Privacy Officer is investigating.

Incident Update

08/04/10:
Veteran B will receive a letter of notification.

NOTE: There were a total of 12 Mis-Handling incidents this reporting period. Because of repetition, the other 11 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The notification letter was sent to Veteran B.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0371902	Missing/Stolen VA Resources	VISN 07 Birmingham, AL	8/5/10			Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/5/2010	INC000000105502	8/4/2010		N/A		N/A	

Incident Summary

The VA Medical Center Research area is under renovation. Some of the researchers are temporarily located at the University of Alabama at Birmingham (UAB) (alternate site approval in place). A VA computer housed at UAB and not on any VA network was recently identified as non-functioning. A call was placed to VA facility OI&T to retrieve the PC from the affiliate office space. Once returned to OI&T, IT staff opened the PC to find that the hard drive and RAM had been removed from the PC. The PC was reviewed in February 2009 by the ISO, Research Compliance Officer, and Privacy Officer and it was confirmed that its use was for storage of non-sensitive information. The Principle Investigator's (PI) practice was to not store data on the local hard drive but to store the de-identified data on a server. The study was last reviewed by the ISO, Research Compliance Officer, and Privacy Officer on 5/19/2010 during a research compliance audit, and at this time no changes to the use of the PC or the PI's practices were determined to have occurred. Thus, it is unlikely any sensitive date is stored on the hard drive.

Incident Update

09/02/10:
The drive was not found. The ISO and CIO will meet with the UAB IT Assistant VP to discuss pulling the remaining VA computers out of UAB.

09/03/10:
The Research renovation is nearing completion and all but four (4) of the investigators will return to VA space. Of the 4 Investigators not returning to the VA, two of the four have already turned in their computers. The total number of computers off-station has dropped to 11. An email was sent to each investigator regarding the event and reminding them of their responsibility associated with the protection of VA equipment. "VA property" will be more clearly labeled on the computers.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0373173	Privacy	VISN 03 New York, NY	8/9/10			Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/17/2010	INC000000107228	N/A		N/A		N/A	

Incident Summary

It was observed that an open computer looked as if it was logged into an external application's website. The employee reported that they possibly saw individuals full last name, first initial, partial social security number and medical information. The PO and ISO at the campus immediately responded once the information was reported. They are trying to find the employees involved and determine if there is any Veteran information on the site now.

Incident Update

08/20/10:
It has been reported that several VAMC's residents and employees have been using the external applications website to store unsecured patient information. It has since been reported that other VAMC's have employees that have also been using the web application for purposes such as tracking change-of-shift reports and tracking lab documents. VHA is conducting a data call to discover the scope of use for this and other similar applications, with a completion date of August 26, 2010. The goal is to determine which Medical Centers have used an external application. The NSOC has blocked web access to this external application website. It is being reported that some users have discovered a way to go around the blocked web site and reach this external application from the VA Network and this is being actively researched and rectified by the NSOC. A ban on all field facility use of these types of applications was discussed on the weekly VHA national hotline call.

08/24/10:
The full national DBCT met and decided that notification will be offered to Veterans whose medical information was posted on the external application, based on the potential disclosure to people without the legal authority for this information. Since the possibility exists that some people who had access to this information are no longer VA residents, VA met the "unauthorized disclosure or access" requirement under both the HIPAA Privacy Rule and VA PL 109-461. So far, it doesn't seem to rise to the level of a "significant risk" required by the HITECT Act. The local ISOs and POs will continue working with the residents to use the information currently stored on external application to determine the number and identity of the Veterans affected.

08/27/10:
Key personnel from the Secretary's Office, OI&T, OGC, and VHA met to discuss next steps. OI&T will be providing instructions on how to get access to the documents that were stored on external application for review. These documents will be reviewed to determine exactly how many Veterans are involved, and exactly what PHI or PII was included. Due to the complexity of this incident, the multiple sites involved, and the varying uses of external applications at many of the facilities, an exact timeline for resolving this incident and notifying Veterans has not been made.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0373913	Privacy	VISN 19 Grand Junction, CO	8/11/10			Moderate	0
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/11/2010	INC000000106331	N/A		N/A		N/A	66

Incident Summary

The employee's locker rooms were closed for renovation. Police, union staff and others were cleaning out the existing lockers prior to demolishing the area and found 2 sheets of paper in a locker that was not locked. The sheets were census sheets from the Community Living Center.. The sheets contained the name and PHI of 41 Veterans and 15 employees. There was no SSN or date of birth on the sheets.

Incident Update

08/12/10:
The 41 Veterans and 15 employees will receive notification letter.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0374560	Privacy	WASHINGTON DC-NCA - 101 Washington, DC	8/12/10			Moderate	218
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/12/2010	INC000000106558	N/A		N/A		N/A	0

Incident Summary

NCA employees found boxes of documents located in a vacant cubical in the NCA Central Office. The boxes contained P-31 forms (Personnel Roster), employee travel documents with full social security number, names, addresses and financial documents listing employee's salaries.

Incident Update

08/13/10:
The documents were left by a former staff member who left in January 2010. The boxes had no markings and were covered with lids but were not secured. The total number of individuals involved is 218 and the information included name and DOB or full SSN. The 218 employees will receive a letter offering credit protection services.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0374838	Missing/Stolen VA Resources	VISN 01 West Haven, CT	8/13/10			Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/13/2010	INC000000106686,	N/A		N/A		N/A	

Incident Summary

A Dell Optiplex 780 PC is missing. The monitor, keyboard and mouse were left on the desktop. The hard drive was not encrypted.

Incident Update

08/24/10:
The ISO discovered the PC missing from a room where residents and interns went to access VISTA and CPRS. The room is located on a patient ward and is not locked. The area has a moderate amount of foot traffic that consists of staff, patients and visitors. There are no cameras in the area. All users sign the Rules of Behavior and are instructed to save data to the network share drives.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0379823	Missing/Stolen VA Resources	VISN 07 Birmingham, AL	8/26/10			Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
8/26/2010	INC000000108571	8/25/2010		N/A		N/A	

Incident Summary

On 08/20/10, an IT specialist prepared to load VA software onto several brand new laptops in a secure storage room within OIT space and then left for the day. When he returned to retrieve the the laptops on 08/24/10, one laptop was missing. The employee and several colleagues searched the area. The CIO was notified and OIT management had all hands search the entire OIT area and the item was not found. The IT specialist had not yet loaded the encryption software onto the laptop. The laptop was officially inventoried on 08/09/10. The missing laptop was reported to VAPD.

mber of lost Blackberry incidents	12
Total number of internal un-encrypted e-mail incidents	65
Total number of Mis-Handling Incidents	59
Total number of Mis-Mailed Incidents	115
Total number of Mis-Mailed CMOP Incidents	6
Total number of IT Equipment Inventory Incidents	8
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	10 (7 encrypted, 1 brand new)